Trabalho de investigação - Revista Redes nº83, de Março de 2002

Sandrina Freitas Duarte nº5221
Engenharia Informática
Escola Superior de Tecnologia de Tomar

14 de Novembro de 2002

Prefácio

A revista **Redes** é especializada, como o nome o indica, em redes de dados. Os leitores da revista são informados sobre novas tecnologias e novos produtos no mundo da rede, através de artigos, todos em português.

No âmbito da cadeira de Redes de Dados II, do terceiro ano, do curso de Engenharia Informática, foi proposto aos alunos de efectuar um trabalho de investigação, comentando alguns artigos de uma revista Redes, escolhida pelo aluno. Assim, cada aluno terá de explicar os artigos que lhe parecem mais importantes para a cadeira. A revista Redes nº83, de Março de 2002, foi a edição escolhida para a realização do minha investigação.

A capa da revista tem como principal título "*Peer-to-Peer* chega às empresas". Serão então uns dos artigos que deverá ser comentado, assim como o artigo tutorial que se refere ao standard 802.11x, que segundo a revista está a "ganhar terreno no wireless".

Percorrendo a revista, encontramos vários artigos interessantes que falam de temas importantes da actualidade, como o artigo relacionado com o wireless, ou mais precisamente da mobilidade que é cada vez mais procurada num sistema de rede. Outro artigo também relacionado com a mobilidade é o artigo que detalhe os novos objectivos da 3Com no que concerne este assunto.

Continuando a consulta da revista, aprendemos que os PDAs poderão futuramente combater fogos. Mas como um simples PDA pode combater fogos? Será interessante explicar a tecnologia que permite efectuar esta prevenção. Outro tema também interessante é o das WAN(*Wide Area Network*). Trata-se da instituição DGO que decide-se lançar na aventura das **WAN**. Será explicado mais a frente, no desenvolvimento deste artigo, o objectivo e os novos projectos desta instituição.

O serviço de voz é também um tema proposto pela revista. O artigo correspondente explica o avanço de Portugal neste sector e as tecnologias utilizadas neste domínio. Um artigo também importante, bastante completo, fala de alguns padrões Web que estão tentando impor-se na área das empresas. Quais

são esses padrões Web? Serão mencionados explicando o seu funcionamento no desenvolvimento. E por fim, será abordado o tema das infra-estruturas IP.

Conteúdo

Lista de Figuras

Capítulo 1

Editorial

Página 16, por P. Ribeiro

No seu editorial, Paulo Ribeiro, director da revista **Redes** refere-se à tecnologia ***Peer-to-Peer*(P2P)**, tema abordado na revista e que ocupa um lugar importante na capa. O director precise que esta tecnologia não é uma tecnologia recente. Efectivamente, o P2P já existe há 30 anos. É agora uma tecnologia muito em voga. Mas porquê que só agora é que esta tecnologia já foi adoptada por muitos? Porque os custos e preços de processamento e de largura de banda são mais acessíveis.

É definido de maneira muito sucinta o P2P, como "uma tecnologia que permite a partilha directa de recursos e serviços entre sistemas ligados entre si". Será explicado em mais profundidade esta tecnologia no desenvolvimento do artigo "P2P desperta atenções". O director também menciona que esta tecnologia tem uma aplicação essencialmente informática, como por exemplo no desenvolvimento de programas capaz de serem executados em simultânea por vários computadores ou a partilha de conteúdos entre computadores encontrando-se a grande distância. É mencionada um série de aplicações desta tecnologia, como por exemplo, jogos on-line. São muitos os adeptos que se ligam à Internet para jogar em rede. É uma prática muita corrente. Outra prática também muita corrente é a partilha de ficheiros áudio. Quem não ouviu falar dos ficheiros mp3 e do *Napster*?

Esta técnica não é só utilizada por utilizadores comuns, é também utilizada por empresas. Mas como é referido neste editorial, são necessários alguns cuidados ao lidar com esta tecnologia. Ao partilhar ficheiros e informação, não é garantido a segurança. Uma empresa mundialmente reconhecida não se pode permitir de utilizar o P2P sem aplicar certos conceitos de segurança. Poderia ter consequências irreparáveis e custosas. E este tipo de segurança não pode ser assegurada por simples *firewalls* ou soluções NAT. E porquê? Porque, como o

Paulo Ribeiro o diz, "as aplicações P2P empacotam os seus pacotes específicos no protocolo de comunicação *Web*, que funciona como via de entrada".

Em conclusão deste editorial, o director da revista insiste no facto de a segurança ainda ser um problema no uso desta tecnologia. Algumas aplicações que respeitam a segurança já foram elaborados. Esta responsabilidade de manter a segurança é da responsabilidade dos fabricantes de soluções de segurança.

Capítulo 2

Mobilidade atrai atenções

Página 16, por S. Esteves e J.P. Faria

Hoje em dia, o que os utilizadores de redes procuram, é mobilidade. Isto quer dizer, poder aceder a informações através de redes, mas não estando ligado por meio de fios a outros sistemas de rede. Esta noção de mobilidade é mais conhecida por ***wireless***.

O objectivo do *wireless* é permitir a um utilizador desta tecnologia, aceder a mesma informação (ou quase toda), que um utilizador ligado a uma rede LAN ou a *Internet*.

Este artigo trata de explicar como o *wireless* está a levantar muitos interessos por parte de utilizadores que não podem sempre estar perto de um computador ligado a uma rede de dados, e por parte das empresas, mais particularmente relatando a posição da famosa empresa **Siemens** em relação à tecnologia *wireless*.

2.1 O que é o *wireless*?

O *wireless* é um sistema de redes sem fios. Este sistema utiliza um dispositivo de cartas integradas, que permitem ter um acesso de rede sem estar ligado até a um *hub* ou a uma linha telefónica com a ajuda de um fio. Permite ao utilizador de trabalhar onde ele quer.

2.2 WAP

A tecnologia **WAP** tem por objectivo de permitir a terminais móveis (por exemplo, telemóveis) de aceder a documentos transmistidos pelas redes sem fios. Permite então que qualquer terminal móvel posse formatar documentos.

Foi então concebido um protocolo universal: o **WAP** (*Wireless Application Protocol*). Este protocolo define a maneira de um terminal aceder a serviços *Internet* e a maneira de estruturar os documentos, graças a uma linguagem derivada do **HTML**, designado **WML** (*Wireless Markup Language*) e uma linguagem de *script*, chamado **WMLScript**.

Com a aparição de redes sem fios, era necessário disponibilizar serviços *Internet* móveis. Mas aparaceram restrições como a passa-banda reduzida e o terminal (ecrã reduzido, memória em pequena quantidade, fraca capacidade do processador, etc.). Era então necessário implementar um protocolo específico a estes terminais.

A tecnologia WAP deve permitir o acesso a serviços *Web*. Um servidor WAP é muito semelhante a um servidor *Web*, mas a maneira de aceder a este sevidor é que é diferente. O acesso a um servidor WAP por um terminal móvel tem três actores:

- o terminal móvel
- o servidor WAP (fornecendo os serviços)
- um *gateway*, servindo de interface entre o terminal móvel e o servidor

O funcionamento da transacção

O terminal móvel (um dispositivo móvel, como por exemplo um telefone com funcionalidades do WAP, um **PAD**, ou outro dispositivo compatível com esta tecnologia) desejando obter dados de um servidor WAP, tem que se ligar a um *gateway* graças a um número de telefone, ou com um assistente de ligação que efectuará a chamada. Quando o terminal móvel está ligado ao *gateway*, o conjunto das transacções, efectuadas pelo terminal, é transmitido pelo *gateway* ao servidor WAP por uma transmissão de tipo IP, semelhante às pesquisas do HTTP.

O servidor responde ao *gateway* por documentos com o formato WML (a linguagem de formatagem dos documentos para terminais móveis), segundo a pesquisa do terminal móvel. Uma vez que os dados se encontram formatados, o *gateway* transmite-os ao terminal móvel por intermédio de uma rede sem fios.

Num primeiro tempo, o *gateway* tem um papel de interface entre o terminal, funcionando como uma rede sem fios, e a rede IP, funcionando com qualquer suporte. Mas o *gateway* tem outra função. Permite transformar as respostas do servidor em dados binários compactados, muita mais adaptados à transmissão por rede sem fios, com passa-banda mais fraca. Quando o terminal recebe os dados, este descodifica-os com a ajuda de um circuito destinado a este efeito.

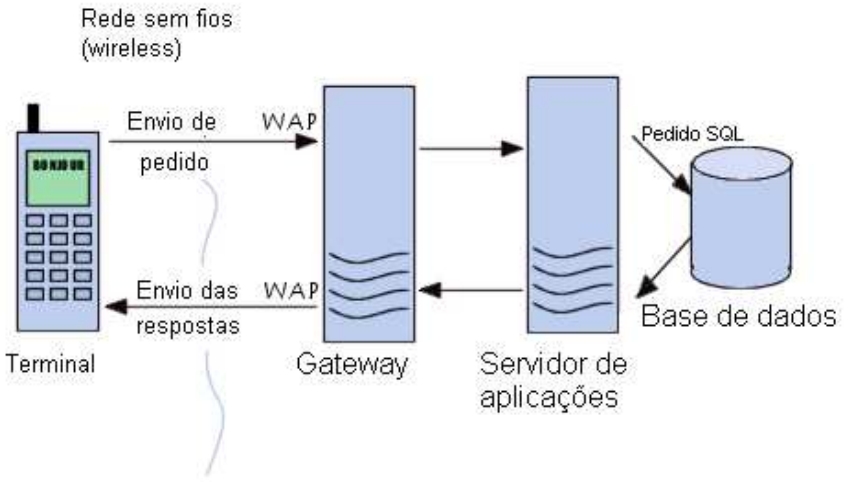

Figura 2.1: Transacção do WAP

As camadas WAP

O protocolo WAP é definido com camadas (como o protocolo OSI) afim de separar os diferentes tratamentos dos dados necessários para efectuar transacções. Esta técnica permite implementar as camadas de um modo diferente. Assim, cada camada define um interface para a camada superior.

O protocolo WAP é composto por cinco camadas:

- camada WAE (*Wireless Application Environment*), camada de aplicação
- camada WSP (*Wireless Session Protocol*), camada de sessão
- camada WTP (*Wireless Transaction Protocol*), camada de transacção
- camada WTLS (*Wireless Transport Layer Security*), camada de segurança
- camada WDP (*Wireless Datagram Protocol*), camada de transporte

Camada WAE (*Wireless Application Environment*)

A camada de apliação do WAP define o ambiente de desenvolvimento das aplicações nos terminais móveis. Fornece assim algumas funcionalidades, tais que, o **WML**, o **WMLScript**.

Camada WSP (*Wireless Session Protocol*)

Figura 2.2: Camadas do protocolo WAP

Esta camada propõe dois protocolos: um protocolo orientado à ligação (estabelecimento de ligação, envio de dados, encerramento de ligação: os dados chegam na mesma ordem que foram transmitidos) e um protocolo não orientado à ligação (a ordem de chegada não é garantida). A existência destes dois protocolos permite beneficiar quer de longas sessões sem encerramento, na qual a comunicação pode ser interompida e reiniciada, quer sessões iniciadas pelo servidor.

Camada WTP (*Wireless Transaction Protocol*)

Esta camada gere o desenvolvimento da transacção, define portanto a fiabilidade do serviço. A comunicação pode ser efectuada de três maneiras diferentes: sentido único sem encerramento, sentido único com encerramento e full-duplex.

Camada WTLS (*Wireless Transport Layer Security*)

Para transmitir dados no ambiente sem fios, é necessário assegurar um nível de segurança nas transacções. Esta camada é responsável pela seguramça e é baseada no standard SSL, Secure Socket Layer (tema abordado noutro capítulo). Permite criptar as trocas de dados, garantir a integridade dos dados (verificar se estes não foram modificados), autenticar os actores da troca.

Camada WDP (*Wireless Datagram Protocol*)

Esta camada é a base da pilha de protocolos WAP. É encarregada de efectuar o interface com os protocolos de transmissão de dados e os operadores dos serviços WAP: GSM, GPRS, UMTS, etc.

2.3 UMA - *Universal Multimedia Access*

A Siemens elaborou um projecto, designado UMA (*Universal Multimedia Access*), que permite transformar documentos construídos com a linguagem HTML, em documentos implementados com a linguagem WML. O UMA é uma aplicação que permite o acesso a conteúdo multimédia sem que o autor tenha de criar uma versão do conteúdo para cada tipo de terminal. O UMA cria dinamicamente a versão do conteúdo adequada ao terminal utilizado.

Mas a Siemens está preocupada em fornecer aos utilizadores do WAP, as mesmas funcionalidades, ou a quase todas, que um posto de trabalho pode fornecer, o que pode parecer bastante complicado devido por exemplo ao tamanho do ecrã. Assim, o UMA identifica o terminal que está a querer aceder a dados a partir do WAP, e sabendo as características do terminal, o UMA poderá então iniciar um processo de redimensionamento dos dados, de maneira a que os novos conteúdos sejam compatíveis com o terminal.

O UMA é apenas uma solução capaz de transformar documentos de uma linguagem para outra. Temos que ter em mente, que esta solução não permite formatar páginas. O UMA não substitui um portal criado de raíz. O WAP *Portal Builder* é uma ferramenta que poderá criar um formato de página que pode ser interpretado pelo *browser* a partir de conteúdos transformados. Uma empresa decide quais são os conteúdos HTML que esta deseja disponibilizar aos utilizadores do WAP. Por outras palavras, conteúdos HTML seleccionados serão transformados para WML.

Outra área que está a interessar a Siemens é o ***video streaming*** para um uso publicitário. O *Video Streaming* é uma aplicação que permite a visualização de vídeo em qualquer terminal (fixo ou móvel). Por exemplo, quando um utilizador está a visualizar um evento em directo, o servidor irá inserir uma *frame* de publicidade. Esta aplicação poderá também ser utilizada para aceder remotamente a câmaras de vigilância que existam dentro de casa. Outro exemplo de

visualização, consiste no *preview* de filmes de cinema. Noutra área, a Siemens é a única, no mercado do GSM, a oferecer a possibilidade aos programadores, em ambientes móveis, de utilizar um software de desenvolvimento **Java**.

A Siemens está a apostar imenso nas soluções utilizadas em ambiente sem fios. Espera, com o desenvolvimento destes produtos, liderar o mercado de redes sem fios, para disponibilizar aos clientes os mesmos conteúdos que um posto de trabalho clássico.

Capítulo 3

3Com ruma à mobilidade

Página 22, por J.P. Faria

3.1 3Com e novos projectos

A 3Com é uma empresa muito conhecida no mundo das redes, mais particularmente no desenvolvimento de novas tecnologias e de novos produtos, e no fabrico de equipamentos, como *switches*, *hubs*, etc. Mas qual é a posição da 3Com face à mobilidade? Este artigo menciona as novas tecnologias da 3Com, relacionadas com a mobilidade, ainda em estado de teste ou já inserido no mercado das redes.

A 3Com está essencialmente preocupada em desenvolver produtos para empresas, mas que respeitam cinco pontos, importantes hoje em dia, para o crescimento das redes empresariais.

Uma das preocupações da 3Com é assegurar um nível de segurança mínimo. Efectivamente, a segurança é uma questão muito importante para redes empresariais. Uma empresa não pode permitir perdas de informação no interior da rede. Os conteúdos que só podem circular no interior da empresa não podem ser acedidos pelo exterior. Para garantir esta segurança, a 3Com está a desenvolver *firewalls* e *filtering* nos *switches*.

3.2 O que é um firewall?

Um computador ligado à Internet ou qualquer tipo de sistema pode ser a qualquer momento vítima de uma intrusão, podendo comprometer a integridade do sistema ou alterar alguns dados. Surge então a necessidade para as empresas conectadas à Internet, de instalar um sistema de *firewall*.

Um *firewall* é um sistema física ou lógica, que serve de interface entre um ou mais conjuntos de redes. Este sistema controla, e eventualmente pára, a circulação de pacotes de dados, analisando as informações contidas nas camadas 3, 4 e 7 do modelo OSI. O *firewall* é composto , no mínimo, por dois interfaces: um para a rede a proteger e outro para a rede exterior.

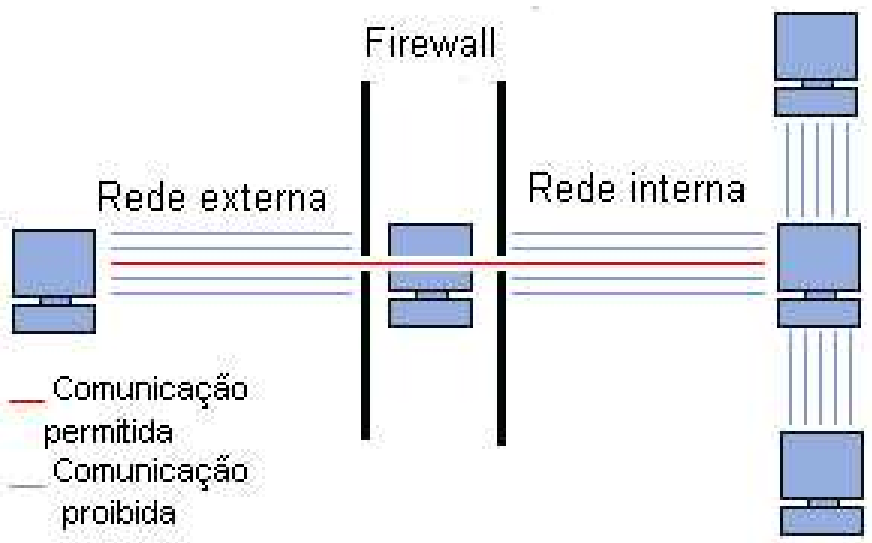

Figura 3.1: Componentes de um firewall

Nas empresas, o *firewall* é geralmente um dispositivo à entrada do sistema de rede e permite proteger o sistema de qualquer intrusão proveniente das redes externas.

Quando algumas máquinas da rede precisam de ser acedidas do exterior(servidor FTP, servidor de mail,...), surge a necessidade de criar um novo interface, incluído num outro sistema de rede, acessível tanto do exterior como do interior, sem comprometer a segurança da empresa. Este sistema de rede é designado por DMZ(DeMilitarized Zone).

O funcionamento dum *firewall*: a filtragem dos pacotes

O funcionamento dos *firewalls* é baseado na filtragem dos pacotes IP, trocados entre duas máquinas. Quando uma máquina exterior se liga à uma máquina da rede local, os pacotes de dados são analisados pelo *firewall*. Estes pacotes são constituídos por:

- o endereço IP da máquina de origem

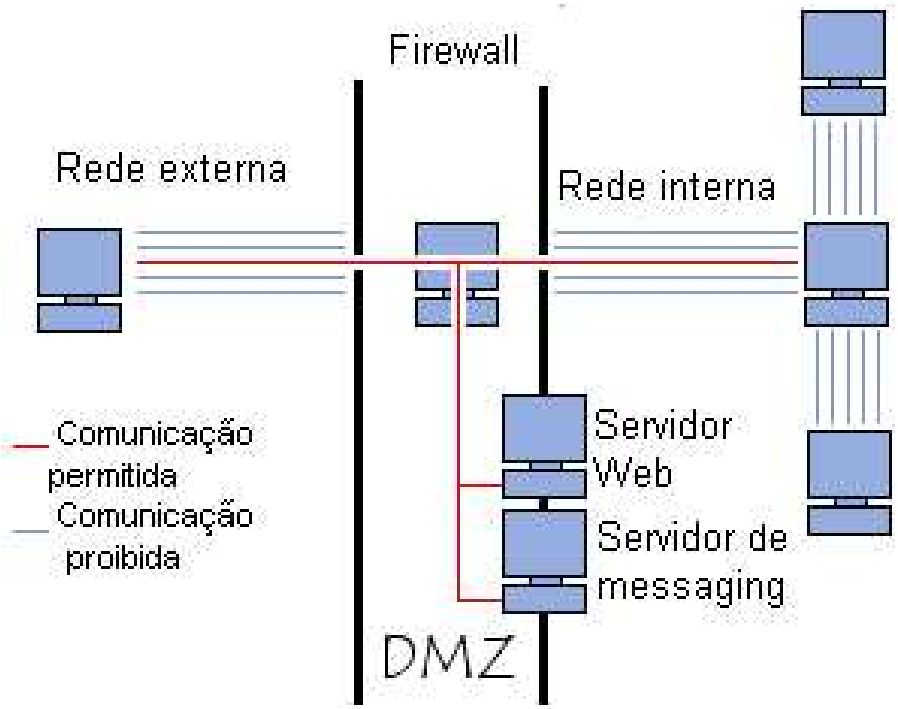

Figura 3.2: Componentes de um firewall

- o endereço IP da máquina de destino
- o tipo de pacote(TCP, UDP,...)
- o número associado ao servico(25 e 110: correio electrónico, 80:http)

Quando a filtragem é baseada nos endereços IP, este filtragem é chamada **filtagem por endereços**(***adress filtering***), enquanto a **filtragem por protocolo**(***protocol filtering***) é baseada na análise do tipo de pacote e do número do serviço.

O *firewall* também analisa as camadas 4 e 7 do modelo OSI, permitindo controlar as transacções entre servidor e cliente, e filtrar as comunicações de tipo aplicação por aplicação.

Voltando as soluções da 3Com, esta também está interessada na norma 802.1x, no que diz respeito ao login em redes *wireless* deste tipo.

3.3 Norma IEEE 802.1x

As redes de dados são frequentemente alvo de ataques de *Hackers*. Mas, nem sempre estas intrusões são feitas através da *Internet*. Muitas vezes, os intrusos utilizam a própria estrutura tecnológica da rede. Isto acontece porque a maioria das redes não possui mecanismo de controlo de acesso, o que facilita o trabalho de pessoas não autorizadas, mas que possuem acesso físico à rede, para executar uma série de ataques.

Esta vulnerabilidade está presente em redes sem fios, e permite utilizadores, não autorizados, acederem a serviços da rede. Como por exemplo, universidades, indústrias, hotéis e aeroportos, porque não possuem um controlo de acesso aos serviços de rede.

Para assegurar que as redes LAN estão a ser utilizadas apenas por utilizadores autorizados, surgiu o padrão IEEE 802.1x que define um novo tipo de segurança de acesso, que requisita a todos os utilizadores uma prévia autenticação antes da disponibilização dos recursos e serviços da rede. Embora existem métodos de autenticação que já foram aplicados no controlo de acesso à rede, no passado, a maioria deles era baseado em MAC *Address* das estações, isto é, os dispositivos eram autenticados, mas o utilizador deste dispositivo não era identificado.

O método do 802.1x é totalmente baseado na identificação e autenticação do utilizador, utilizando servidores de autenticação para executar esta identificação.

3.3.1 Terminologia

Estas terminologias são utilizadas nas redes de tipo IEEE 802.1x:

- Servidor de autenticação - este é o agente responsável pelo processo de recepção e resposta de solicitações, para autenticação de acesso à rede.
- Autenticador - *Switch*, router ou ponto de acesso que disponibiliza o acesso aos utilizadores da rede. Estes dispositivos são responsáveis pela autenticação do acesso à rede
- *Supplicant* - Dispositivo de rede que necessita ser autenticado na rede. Na maioria dos casos são estações de trabalho, mas podem ser também *switches* que devem ser autenticados por outros autenticadores.
- EAP - *Extensible Authentication Protocol*. EAP é um protocolo genérico que permite que os pontos de acesso à rede suportem múltiplos métodos de autenticação.

3.3.2 Descrição do 802.1x

Quando implementado o 802.1x na rede, um *supplicant* deve em primeiro ser autenticado pelo agente autenticador que fornece o meio de acesso à LAN. O autenticador mantém um controlo do status da porta para cada *supplicant* que ele está a examinar, e no caso do *supplicant* ser autenticado, então a porta passa para o status autorizado, e o *supplicant* pode enviar os dados da aplicação para a LAN através do *Network Access Server* - **NAS** (*switch* de acesso). Porém quando o *supplicant* não é autorizado, o status da porta no autenticador permanece como não autorizado, e o *supplicant* não consegue enviar dados de sua aplicação através do *Network Access Server*).

Quando o NAS detecta uma actividade na porta, ele envia um EAP-*RequestID* para identificação do utilizador do dispositivo. O EAP é um protocolo de autenticação que é executado antes da transmissão de outros protocolos. Quando o dispositivo recebe esta requisição (e possui um client 802.1x instalado), ele responde com a sua identificação para o autenticador, que por sua vez encaminha a mesma, para um servidor de autenticação. Neste caso, o servidor de autenticação trabalha como um identificador e fornecedor de perfil de acesso, através do qual o utilizador pode estar em localidades diferentes, porém tendo o mesmo perfil dentro do mesmo servidor de autenticação.

Em resposta ao *AccessRequest* o servidor de autenticação envia ao autenticador um *AccessChallenge*, e o NAS neste momento, encaminha EAP-*Request* para o dispositivo que, por sua vez, responde com um EAP-*Response*, com a identificação do utilizador. Então o NAS encaminha esta identificação do utilizador para o servidor de autenticação, que determina se o mesmo possui acesso ou não à rede, baseado na sua identificação. No caso do utilizador ser identificado, é enviado um *Accept* para o NAS, que por sua vez encaminha um EAP-*Success* para o dispositivo, autorizando a transmissão de dados na respectiva porta do utilizador.

Este processo é inicializado cada vez que houver uma mudança de estado up/down na porta, isto significa que caso o utilizador desliga o seu dispositivo da porta, todas as configurações serão perdidas, sendo necessário a repetição de todo o processo de autenticação.

Outro facto que levanta interesso por parte da 3Com é a mobilidade como já foi referido anteriormente. A 3Com quer fornecer às empresas um serviço de *wireless* baseado nos standards 802.11a e 802.11b. Antes de seguir o desenvolvimento das novas soluções da 3Com, é necessário explicar brevemente o que são os 802.11a e 802.11b. Mas não vamos entrar em detalhes porque este tema é abordado noutro artigo.

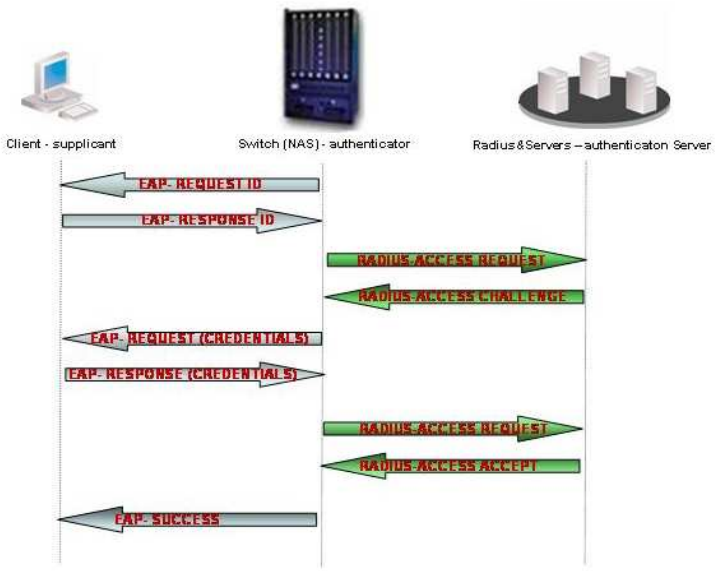

Figura 3.3: Funcionamento do 802.1x

3.4 IEEE 802.11x

Novas tecnologias têm surgido para atender diferentes necessidades de redes sem fios. Em 1997, a elaboração do standard IEEE 802.11 para as redes sem fios foi um passo importante no desenvolvimento de tal sistema. Esta norma foi desenvolvida para favorecer a interpolaridade do material de diferentes fabricantes. Esta norma dita as condições a respeitar para a elaboração de uma rede sem fios.

A empresa 3Com quer permitir uma coexistência entre o 802.11a, que permite débitos de 54 Mbps, e o 802.11b, com um débito de 11Mbps. Esta coexistência será levada até as soluções de telefonia NBX IP da 3Com. Esta tecnologia é uma tecnologia de telefonia LAN com suporte LAN Ethernet/IP.

3.5 Outros projectos

A terceira aposta da 3Com relaciona-se com as LAN: oferecer uma gama completa para instalações LAN, como por exemplo chassis escaláveis e modulares. A 3Com também está interessada em adoptar o 10 Gigabit Ethernet, no objectivo de harmonizar os preços.

A 3Com pretende também melhorar o acesso a conteúdos localizados em servidores. Para isso, será necessário aumentar a velocidade de transmissão ao utilizador, o que consiste em reduzir os custos relacionados com o equipamento das WAN (Wide Area Network).

Finalmente, o último objectivo será de melhorar as comunicações, directas ou indirectas entre utilizadores no interior de uma rede LAN, utilizando a tecnologia NBX da 3Com e serviços de *messaging* (voicemail, e-mail, fax). Estas aplicações também terão de ser disponíveis em redes *wired* ou *wireless*.

Estes novos projectos da 3Com tem por objectivo de diminuir os preços relacionados com a transmissão de dados sem fios e de disponibilizar serviços de utilização fácil para os clientes.

Capítulo 4

PDAs combatem fogos

Página 27, por F. Rocha

Os fogos florestais continuam a ser um grande problema em Portugal. Todos os anos são registados centenas de fogos deste tipo. Estes fogos tornam-se muitas vezes difíceis de controlar devido à falta de informação no terrno. Para remediar a este problema, a ESA (Estação Espacial Europeia) lançou um concurso, em Junho 2001, limitado à industria portuguesa, como objectivo de obter uma solução baseada nos sitemas de informação e na mobilidade. A empresa escolhida foi a CRITICAL SOFTWARE, sediada em Coimbra, tendo como subcontratado o Centro Nacional de Informação Geográfica (CNIG).

O PREMFIRE (*Prevention and Mitigation of Fire Hazard in Portugal*), nome dado a este projecto, tem como objectivo alargar as potencialidades do sistema RISE (Rede de Informação de Situações de Emergência), existente no Serviço Nacional de Protecção Civil (SNPC).

O sistema actualmente em funcionamento permite gerir o planeamento e a resposta a situações de emergência em todo o país, nomeadamente ao nível da mobilização de meios. Mas, o RISE era aplicável a computadores tradicionais. Surgia o problema de este sistema não poder ser utilizado pelos bombeiros no terreno. Por isso, serão utilizadas agendas de bolso (PDA) com ligação *wireless*.

O PREMFIRE terá as características do RISE adicionando ao sistema a capacidade de cálculo e inclusão de Cartas de Risco de Incêndio, a emissão de alarmes às unidades de bombeiros das zonas de maior risco, e a utilização no teatro de operações, incluindo mapas, imagens de satélite e informação alfanumérica. Estas informações serão colocados no módulo central, onde os bombeiros poderão se ligar através dos PDAs, para obter informação no terreno. Os PDAs constituirão assim o módulo de terreno.

O software utilizado no módulo de terreno será o *Pocket PC* 2002 da Microsoft, um nova versão de software para PDA (assistentes digitais pessoais).

Para poder garantir a transmissão de informação entre o módulo central e o módulo de terreno, será utilizado a tecnologia GSM/GPRS.

O contrato entre a Critical Software e a ESA é válido até Dezembro de 2002. O PREMFIRE será apenas utilizado como auxiliar no combate aos incêndios. Poderá talvez auxiliar na prevenção de tempestades ou inundações. Este sistema será utilizado pelos agentes do SNPC (Serviço Nacional de Protecção Civil).

Capítulo 5

Padrões Web procuram impor-se

Página 33, por J. Trigo e J.F. Masler

São vários os padrões Web disponíveis no mercado da Internet: HTML, CSS, Java, XML, etc. Mas, como o indica este artigo, alguns padrões tem dificuldades em impor-se nas soluções propostas pela EAI.

5.1 As soluções EAI

Como já foi referido, alguns padrões tentam impor-se nas soluções EAI. Mas afinal, o que são estas soluções? O que é a EAI?

A EAI, em inglês, significa *Enterprise Application Integration*, traduzindo para português, obtemos integração das aplicações empresariais. Novas tecnologias não param de aparecer. E as empresas começam uma intensa busca por sistemas que podem facilitar o seu dia a dia e melhorar o desempenho. O problema é que aparece sempre uma nova aplicação, fazendo com que cada empresa possa adoptar diferentes tecnologias. E como fazer para integrar essas aplicações? Afinal, não adianta muito ter várias novidades para melhorar o desenvolvimento, se as tecnologias que foram implementadas em épocas distintas não conseguem interagir com as suas informações. É para resolver esse problema que surge o conceito de *Enterprise Application Integration* (EAI), um sistema que tem exactamente o objectivo de integrar todas as aplicações da empresa e também da empresa com os seus fornecedores.

Fala-se muitas vezes dos projectos *EAI*(ou soluções EAI), para designar integrações por vezes complexas, entre una nova aplicação e uma já existente.

Tecnicamente, um projecto EAI consiste em abandonar um sistema ponto-a-ponto para passar a adoptar um sistema em estrela, baseado à volta do sistema EAI.

Um exemplo de um standard que tentou abrir um caminho nas soluções EAI foi o XML.

5.2 XML- Extensible Markup Language

O XML é uma linguagem de marcação de dados (estas marcas são chamadas *tags*, semelhante às do HTML), que permite implementar documentos de maneira estruturada. Mas, contrariamente ao HTML, que define a formatação de caracteres e parágrafos, o XML permite também novas *tags*, para estruturar documentos, baseadas mais no conteúdo dos dados, do que na apresentação (HTML). Assim, o XML permite separar o conteúdo da apresentação, o que permite, por exemplo, afixar um mesmo documento sobre aplicações diferentes sem por isso necessitar de criar tantas versões do documento, que necessitamos de apresentações. O XML foi implementado pelo XML *Working Group* dirigido pelo *World Wide Web Consortium* (W3C) desde 1996.

Mas este padrão não teve o sucesso esperado. Não mostrou grande interesso por parte das empresas, que utilizam o EDI em vez de o XML. O EDI é um sistema de intercâmbios automatizado de dados. Este sistema é baseado no comércio electrónico. Embora o ebXML, um padrão mais genérico poderá alterar a situação.

O que parece causar problemas para o XML impor-se nas soluções EAI, é o facto de ser uma linguagem que não tem apresentação. Efectivamente é preciso de outra linguagem para converter os dados apresentados por um documento em XML para poder ver os dados de maneira legível para toda a gente. A transformação dos dados é realizada pelo XSLT.

5.3 XSLT - *Extensible Stylesheet Language Transformation*

Um documento XML pode ser representada como uma linguagem imperceptível. Assim, o XSLT permite transformar os documentos XML com a ajuda de folhas de estilo, que contêm regras designadas *template rules*.

O processador XSLT (componente encarregada da transformação) cria uma estrutura lógica, composta por árvores, a partir do documento XML e efectua transformações segundo as *template rules*, para produzir uma árvore resultado, representando por exemplo a estrutura de um documento HTML.

Outros standards que começam a emergir são o JMS (*Java Message Service*) e o JCA (*Java Connector Architecture*) da plataforma J2EE (*Java 2 Entreprise Edition*).

5.4 J2EE da SUN

J2EE é um servidor de aplicações, que permite construir, a partir de componentes logística, aplicações diversas disponibilizadas ao utilizador. Este tema é abordado com mais pormenores na revista Redes nº87, que será apresentada por outro aluno.

5.5 JMS - Java Message Service

5.5.1 Messaging

Antes de mais, temos que perceber o que é um *messaging*, antes de explicar o que é o JMS. O *messaging* é um método de comunicações entre componentes ou aplicações. Existem dois tipos de *messaging*: o *peer-to-peer*, com serviço centralizado para repasse de mensagens enviadas e recebidas, e o MOM. O MOM é um serviço central de mensagens que administra canais aos clientes e servidores para enviar e receber mensagens. O MOM ignora os conteúdos e o formato das mensagens.

5.5.2 JMS

Agora, já é possível explicar o que é o JMS. O JMS é um interface Java única para unir os MOMs incompatíveis. Pode ser definida como um interface para criar, enviar, receber e ler mensagens através de um MOM. O seu objectivo é oferecer um interface simples, unificado e compatível com aplicações existentes (não JMS), suportar mensagens contendo objectos serializados Java e páginas XML. É um modelo flexível de desenvolvimento baseado em dois domínios: ponto-a-ponto e publicação-subscrição. Em relação à plataforma J2EE, é suportado por todos os servidores de aplicação J2EE.

Ponto-a-ponto O domínio ponto-a-ponto é baseada no conceito de filas, remetentes e destinatárias. Cada mensagem é enviada para uma fila específica e é consumida por um destinatário (que pode ou não estar disponível no momento). O destinatário confirma que a mensagem foi recebida e processada correctamente (*acknowledgement*). As filas retém mensagens até que sejam consumidas.

Publicação-subscrição Esta versão é baseada em canais (tópicos). É uma comunicação muitos para muitos: as mensagens são enviadas a um canal onde todos os assinantes do canal podem retirá-las.

5.6 JCA - *Java Connector Architecture*

A JCA foi desenvolvida pela SUN, no âmbito de criar uma interpolaridade universal das aplicações. O seu objectivo principal é de definir uma camada de standards permitindo a um servidor Java de dialogar com as aplicações baseadas noutras tecnologias. Com a JCA, a Sun quer facilitar o desenvolvimento de interfaces de conexões e de adaptadores standards. A JCA e os serviços Web podem ser comparados em termos de arquitectura.

Resultado, com JCA, acabarem as bibliotecas de centenas de conectores para responder às características tecnológicas de cada arquitectura de integração. Dum lado, os fornecedores de serviços e de soluções EAI terão apenas a missão de desenvolver um interface standard para criar as chamadas afastadas e integrar a linguagem de contrato necessário. Do outro lado, o trabalho dos editores de soluções será apenas de desenvolver um adaptador único para abrir caminho a plataforma J2EE. A JCA pode assim oferecer uma melhor escolha de soluções de empresas.

O JCA, contrariamente ao XML, parece integrar as soluções EAI. O JCA corresponde ao único standard que define a arquitectura dos conectores que ligam os servidores de aplicações às aplicações empresariais no domínio EAI.

Já existem muitos produtos baseados na plataforma J2EE da SUN. Os fornecedores estão cada vez mais interessados no desenvolvimento de um tal sistema, como por exemplo a IBM, Sybase Neon, Tibco Sotware, webMethods, BEA Systems, Sotware AG, etc.

Devido a emergência de diversos padrões *Web*, destinados à utilização empresarial, a elaboração de standards tem que ser necessária, com base nas condições da EAI. E isto, para facilitar a utilização destes padrões, pelas empresas, que muitas vezes ficam sem saber qual padrão utilizar para as suas aplicações.

Capítulo 6

802.11x ganha terreno

Página 49, por S. Gomes da Silva

Como já foi referido anteriormente, o *wireless* está a conquistar muitos adeptos. O facto de poder aceder a informação, sem ter de ligar computadores uns aos outros com fios, é efectivamente um factor muito importante.

Quando é instalada uma rede local nas instalações de uma empresa, é preciso um sistema de ligação através de fios, por vezes muito complexo. A elaboração deste sistema torna-se um trabalho um pouco pesado para o desenhador de rede. Mas, também traz outras desvantagens. Por exemplo, se depois da instalação toda feita, alguns computadores têm que ser mudados de sítio, uma parte da instalação também tem que ser modificada.

Com a tecnologia *wireless*, todos estes problemas desaparecem. A instalação de uma rede WLAN (*Wireless Local Area Networks*) torna-se muito mais simples do que uma instalação LAN. Desaparecem assim os fios que ligam os sistemas uns aos outros.

Os fabricantes interessem-se cada vez mais a desenvolver novos standards de WLAN, porque é um sector que ocupa um lugar importante no mercado. Estes standards são muitas vezes baseados em outros padrões já existentes, como o HiperLAN, o HomeRF, o Bluetooth e o 802.11.

6.1 HiperLAN

A HiperLAN (*HIgh PErformance Radio LAN*) foi concebido pela ETSI (*European Telecomunications Standards Institute*). A concepção deste padrão começou em 1992 e foi finalizada em 1997. Uma rede HiperLAN tem que responder as seguintes especificações:

- Débito de 23.529 Mbps
- Área da rede: 100m
- Frequêcia de 5.2 GHz

6.2 HomeRF

A norma HomeRF das redes sem fios foi concebido para uma utilização doméstica. A *Home Radio Frequency* utiliza uma técnica de saltos de frequência de 2.4 GHz com um débito teórico de 1.6 Mbps, numa área de 30 metros. A técnica de acesso utilizada é espectro de saltos de frequância FHSS (Frequency Hoping Spread Spectrum). Suporta também uma topologia cliente/servidor (para partilhar uma ligação Internet) e ponto-a-ponto (partilha de ficheiros entre dois computadores). Mesmo se esta norma permite ligar dois computadores, o HomeRF só faz sentido quando é utilizado um ponto de acesso, que efectua a ligação Internet com altos débitos e a gestão das ligações entre os elementos da rede. Os computadores podem partilhar um único acesso à Internet e comunicar entre si.

Uma das desvantagens do HomeRF é que só permitem pequenos débitos, o que o limite ao uso doméstico. Devido a estes débitos, esta norma fica inadaptada às redes empresariais. Este defeito deverá desaparecer, porque os produtos compatíveis com a norma HomeRF 2.0 poderão fornecer um débito de 10 Mbps ou 20 Mbps. Oferece também características interessantes como canais para voz.

6.3 Bluetooth

Bluetooth é uma nova tecnologia de transmissão sem fios. O seu objectivo é de permitir a comunicação numa pequena área entre vários máquinas e sem cabos, utilizando as ondas de rádio. Este tipo de rede sem fios é também designado por **WPAN** (*Wireless Personal Area Network*). Como o nome o indica, é utilizada para fins pessoais.

Hoje em dia, a inserção de equipamentos informáticos, por exemplo as impressoras, numa rede, torna-se uma tarefa complicada. Esta instalação requere muitas vezes uma configuração complicada e muitos cabos. *Bluetooth* permite ligar um conjunto de periféricos, posicionando-os a menos de 10 metros uns dos outros. Nenhuma configuração é necessária.

A tecnologia *Bluetooth* não permite só a comunicação entre dispositivos informáticos. O *Bluetooth* pode ligar qualquer aparelho electrónico. Esta ligação é possível graças à um *chip* de 9mm de lado. Existem muitos exemplos de

ligações: um computador a uma impressora ou a um telemóvel, ao carro, a um PDA, etc.

Para utilizar a tecnologia *Bluetooth*, os aparelhos electrónicos devem estar equipados com *chip Bluetooth*. Os aparelhos compatíveis com esta tecnologia comunicam utilizando ondas de rádio na faixa de frequência de 2400 a 2483.5 MHz.

O débito teórico é de 1Mbps. O envio das informações efectua-se por pacotes de dados com blocos de controlo. Estes blocos permitem a ligação em rede dos aparelhos, o bom encaminhamento dos dados e a correcção de erros de transmissão. O formato dos pacotes é o seguinte:

72 bits	54 bits	[0-2745]bits
Código de acesso	cabeçalho	Corpo da mensagem

Os 72 primeiros bits servem para a sincronização entre os componentes da rede. Os 54 bits de inicio servem para:

- enumerar os pacotes
- saber qual a máquina que mandou o pacote
- determinar o tipo de pacote
- saber se é necessário de mandar uma mensagem de confirmação
- controlar os erros(CRC)

O corpo serve para armazenar os dados para transportar. Contém geralmente um CRC de 8 ou 16 bits.

6.4 IEEE 802.11

O IEEE 802.11 tem por objectivo de definir redes sem fios de tipo Ethernet. Esta padronização garante a interpolaridade entre produtos de diferentes fabricantes. Este padrão é denominado 802.11, porque o padrão 802 corresponde ao standard Ethernet. Então o 802.11 é uma extensão do 802 mas para redes sem fios. Como o nome o indica, é uma tecnologia com um débito de 11Mbps.

Componentes da arquitectura

A rede local 802.11 é baseada numa arquitectura de células. Cada célula, *Basic Service Set* ou BSS, é controlada por um ponto de acesso, chamado *Access Point* ou AP, que funciona como um *bridge* entre a rede *wireless* e a rede tradicional. As estações de trabalho que comunicam entre si dentro da BSS, são denominados por STA.

Mesmo que uma rede local sem fios possa ser formada por uma única célula, com um único AP, a maioria das instalações serão formadas de várias células, onde os AP são conectados por um sistema de distribuição (chamado *Distribuition System* ou DS), do tipo Ethernet e nalguns casos sem fios.

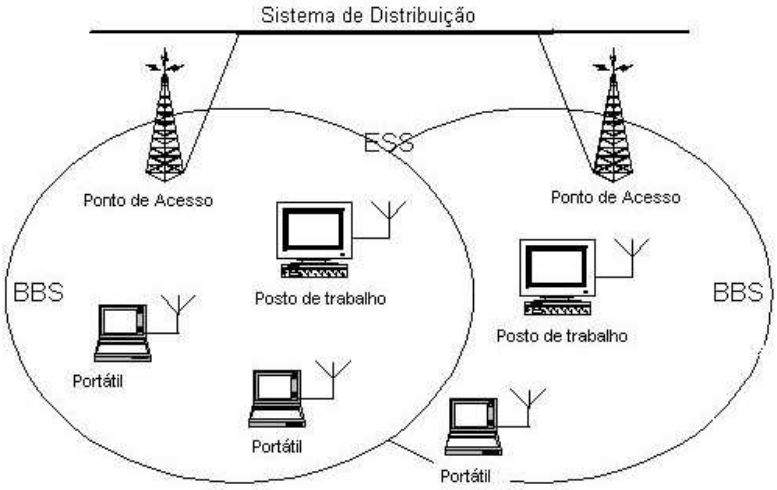

Figura 6.1: Arquitectura de uma rede IEEE 802.11

O conjunto da rede local sem fios inter-conectada, incluindo as diferentes células, os AP respectivos a cada célula e o DS, é visto pelas camadas superiores do modelo OSI como uma única rede 802 e é chamado ESS (*Extended Service Set*). Nestas condições, uma STA pode movimentar-se de um BSS para outro, permanecendo conectada à rede. Este processo é denominado ***Roaming***.

Existem dois modos de operação:

- o modo infra-estrutura: existem pontos de acesso, que coordenam a comunicação entre as estações de uma célula(BSS). Este modo é utilizado no caso dos utilizadores da rede aceder frequentemente à rede central.
- o mode *ad-hoc*: não existe ponto de acesso e as estações comunicam entre si directamente graças a algoritmos, como por exemplo o SEA(*Spoksman Election Algorithm*), mas este modo não é recomendado pelo padrão.

A arquitectura

O IEEE 802.11 estabelece as normas das camadas física(*Physical Layer*) e de ligação de dados (MAC - *Medium Access Control*).

Para a camada física, existem 3 tecnologias diferentes possíveis:

- FHSS - *Frequency Hopping Spread Spectrum*
- DSSS - *Direct Sequence Spread Spectrum*
- IR - *Infrared*

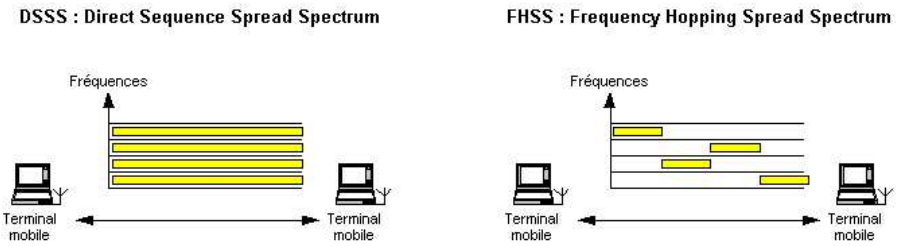

Figura 6.2: Frequências utilizadas

As especificações FHSS e DSSS operam na frequência de 2.4 GHz (banda ISM - *Industrial Scientific and Medical*). Num primeiro tempo, a norma previa para o DSSS, um débito de 2Mbps, enquanto que o débito do FHSS era de 1Mbps. Agora, a nova norma 802.11b, prevê débitos entre os 5.5 e 11Mbps, com a tecnologia DSSS e a norma 802.11a, débitos de 54 Mbps, utilizando a tecnologia OFDM (*Orthogonal Frequency Division Multiplexing*) com frequência de 5 a 5.8 GHz.

A camada MAC 802.11 oferece funções, que geralmente são confiadas a outras camadas: fragmentação, retransmissão de pacotes e envio de confirmação. Existem dois métodos de acesso: o DCF (*Distributed Coordination Function*) e um mecanismo opcional, o PCF (*Point Coordination Function*).

O DCF é também conhecido por CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). O funcionamento do CSMA/CD é o seguinte: se uma estação deseja emitir, esta "escuta"o meio de transmissão. Quando o canal está livre, a estação transmite, caso esteja ocupado, ela aguarda até a transmissão em andamento acabar. Espera um tempo aleatório, calculado pelo o algoritmo *random backoff*, e repita o procedimento de escuta. Quando duas estações querem transmitir ao mesmo tempo, estas provocam uma colisão. Portanto, após a transmissão, a estação aguarda uma confirmação ACK (*Acknowledgement*) da estação receptora. Caso receba um ACK, a transmissão ocorreu com sucesso, caso contrário haverá retransmissão. O ACK é uma garantia que não houve colisões.

Para diminuir a probabilidade de colisões entre estações, a norma definiu um mecanismo de *carrier sense virtual*, cujo o funcionamento é o seguinte: uma estação que deseja emitir, transmite um pequeno pacote de controlo, denominado RTS(*Request To Send*), com informação sobre a origem, o destino e a duração da transmissão. A estação receptora responde enviando um pacote CTS (*Clear To Send*) que inclui a mesma informação de duração. Todas as estações que recebem o RTS ou o CTS, activarão o seu *virtual carrier sense*, durante a respectiva duração. A probabilidade de colisões diminui, porque as estações sabem que durante um determinado período, o meio estará ocupado.

Existe outro modo opcional: a PCF (*Point Coordination Function*), que é utilizado para implementar serviços a tempo real, como a transmissão de voz ou de vídeo.

Fragmentação e montagem de pacotes

Os protocolos de redes locais com fios utilizam pacotes de centenas de bytes (por exemplo, o tamanho dos pacotes Ethernet pode ir até os 1518 bytes). Numa rede sem fios, existem várias causas para utilizar pacotes mais pequenos:

- a taxa de erros por bit é maior neste tipo de meio (ligações radio). A probabilidade de um pacote ser corrompido aumenta com o seu tamanho,
- no caso de um pacote corrompido (por causa das colisões ou mesmo do ruído), menor é um pacote, menor é o *overhead*, durante a sua retransmissão,
- num sistema de saltos de frequência, o meio de comunicação é interrompido periodicamente para a mudança de frequência, portanto menor é o pacote, menor é a probabilidade da transmissão ser interrompida.

Por outro lado, não era necessário criar um novo protocolo LAN incapaz de tratar os pacotes de 1518 bytes utilizados em redes Ethernet. A IEEE decidiu resolver este problema, adicionando um mecanismo de fragmentação e montagem de pacotes na sub-camada MAC. Este mecanismo resume-se a um simples algoritmo de envio e espera de resposta. A estação emissora não é autorizada a transmitir um novo fragmento enquanto:

- não foi recebido um ACK para o fragmento correspondente
- foi decidido que um fragmento foi enviado demais e que a transmissão do pacote seja abandonada.

Inter Frame Space(espaço entre duas frames)

O padrão define 4 tipos de espaço entre duas frames:

- **SIFS** - *Short Inter Frame Space*, é utilizado para separar as transmissões, pertencentes a um mesmo diálogo. É a diferença mais pequena entre dois quadros. Este valor é fixada pela camada física e calculada,
- **PIFS** - *Point Coordination IFS* é utilizado pelo ponto de acesso para conseguir o acesso ao meio antes de qualquer estação. Este valor corresponde ao SIFS mais um certo tempo,
- **DIFS** - *Distributed IFS* é o IFS utilizado por uma estação que deseja começar uma nova transmissão e corresponde ao PIFS mais um tempo,
- **EIFS** - *Extended IFS* é o IFS mais comprido. É utilizado por uma estação, que recebe um pacote que não percebe.

Como é que uma estação se liga a uma BBS?

Quando uma estação deseja aceder a um BBS, a estação necessita de informações de sincronização da parte do Ponto de Aceeso (ou da parte das outras estações no caso de una célula em modo *ad-hoc*). A estação pode obter estas informações de duas maneiras possíveis:

- Escuta passiva: a estação está à espera de receber uma trame, chamada *Beacon Frame*. Esta trame é uma trame enviada periodicamente pelo Ponto de Acesso e contém informação de sincronização.
- Escuta activa: a estação tenta encontrar um Ponto de Acesso, transmitindo uma trame de pedido de pesquisa (*Probe Request Frame*) e espera a resposta de pesquisa do Ponto de Acesso.

O processo de autenticação

Uma vez que a estação encontrou um Ponto de Acesso e decidiu entrar numa célula, é iniciado um processo de autenticação. Este consiste na troca de informações entre o Ponto de Acesso e a estação, onde cada um prova a sua identidade por uma *password*. Se segue a este processo, o processo de associação. Consiste numa troca de informações sobre as diferentes estações e as capacidades da célula. Os Pontos de Acesso guardam a posição actual da estação. Só depois deste processo, a estação pode transmitir e receber trames de dados.

O *Roaming*

O *roaming* é o processo de passagem de uma célula a outra sem acabar a ligação. Esta transição é baseada no envio de pacotes e só pode ser efectuada entre duas transmissões de pacotes. O IEEE 802.11 não especifica como o *roaming* é efectuado, mas define as regras de base: escutas passiva e activa, processo de associação, onde uma estação será associada a um novo Ponto de Acesso.

As estações tem que ficar sincronizadas no interior da rede. Esta sincronização é muito importante para garantir o bom funcionamento das comunicações baseadas em saltos de frequência. Numa mesma célula, todas as estações sincronizam o seu relógio com o do Ponto de Acesso da maneira seguinte:
O Ponto de Acesso transmite periodicamente trames designadas *Beacon Frame*, que contêm o valor do relógio do Ponto de Acesso no momento da transmissão. As estações emissores verificam o valor do relógio no momento da recepção e corrige este valor para ficar sincronizadas com o relógio do Ponto de Acesso.

Segurança

A segurança é um problema que preocupa aqueles que desenvolvem redes locais sem fios. O standard 802.11 define uma solução para este problema: o processo WEP (*Wired Equivalent Privacy*). O mais importante para um utilizador da rede é de ter a certeza que ninguém externo à rede pode aceder aos recursos da rede utilizando o mesmo equipamento sem fios e "escutar"o tráfego da rede (escuta clandestina).

Para prevenir o acesso aos recursos da rede, o standard utiliza um mecanismo de autenticação, onde a estação é obrigada a provar a sua identidade graças a uma *password*. A escuta clandestina é bloqueada com a utilização do algoritmo WEP, que é um método através do qual as mensagens são criptadas.

O protocolo WEP consiste na encriptação de uma mensagem utilizando uma chave k que é compartilhada entre as partes envolvidas na comunicação a fim de proteger o conteúdo da frame de dados. A mesma chave é utilizada para encriptar e decriptar a mensagem. O protocolo WEP tem a intenção de cumprir 3 metas de segurança:

- Confidencialidade: o protocolo deve evitar que intrusos tomem conhecimento do conteúdo das mensagens transmitidas através da rede;
- Controlo de acesso: deve evitar que um intruso utilize a estrutura da rede para enviar ou receber mensagens;
- Integridade dos dados: não pode permitir que o conteúdo das mensagens seja modificado.

Em todos os 3 casos, a segurança apoia-se na dificuldade de se obter a chave que é compartilhada pelas estruturas autorizadas da rede. Existem actualmente duas classes de implementação do WEP: a clássica, e a extendida. A clássica trabalha com chaves de 40 bits, e a extendida, com chaves de 104 bits. A chave clássica é suficientemente curta para tornar os ataques de força bruta possíveis. Entretanto, a chave extendida torna os ataques de força bruta praticamente impossíveis. Mas existem ataques que podem ser feitos com sucesso que não requerem a quebra da chave, o que torna a versão de 104 bits insegura também.

Tipos de frames

Existem 3 tipos principais de tramas: as tramas de dados (transmissão de dados), tramas de controlo (controlar o acesso ao suporte) e tramas de gestão (transmitidas da mesma maneira que as tramas de dados para informações de gestão, mas não são transmitidas às camadas superiores).

Formato das tramas

As tramas 802.11 são compostas pelos seguintes componentes:

Preâmbulo	Cabeçalho PLCP	Dados MAC	CRC

O preâmbulo depende da camada física e contém:

- Synch: sequência de 80 bits alternando 0 e 1, utilizado pelo circuito físico para seleccionar a antena apropriada para corrigir o *offset* de frequência e de sincronização.
- SFD: *Start Frame Delimiter*, série de 16 bits, utilizada para definir o inicio da trama.

O cabeçalho PLCP é transmitido a 1 Mbps e contém informações lógicas utilizadas pela camada física para descodificar a trama.

Aplicações

As soluções baseadas no standard IEEE 802.11 destinam-se a implementação de redes locais sem fio. Diversas áreas podem beneficiar da tecnologia WLAN: hospitais, eventos, escritórios temporários, escolas, etc.

6.5 Outros standards WLAN

802.11g

O objectivo deste standard é de permitir um melhoramento do 802.11b, mas ficando compatível com este. O débito máximo é de 22 Mbps. A entrada deste standard no mercado é previsto para fim 2002.

802.11e

O objectivo deste é oferecer a qualidade de serviço (QoS: Quality of Service) para as redes WLAN 802.11a, b, ou g e permitir assim aplicações como a voz sobre IP (VoIP: Voice over IP).

802.11h

Este standard foi concebido para responder a futuros problemas da sobre-utilização da banda 5.1 GHz (802.11a), que poderia conduzir a não utilização desta. Duas funções são previstas:

- A selecção dinâmica de frequência (DFS:Dynamic Frequency Selection) que permite escolher a banda de frequência a menos utilizada.
- O controlo de potência (TPS: Transmit Power Control) que permite ao emissor de controlar a potência e de emitir à potência necessária. Assim o nível de interferência é mínimo.

802.11i

Este standard deverá resolver os problemas de segurança do WEP, utilizando um sistema de encriptação mais robusto e um sistema de modificação de chaves.

6.6 Qual a melhor implementação de rede sem fios?

Antes de efectuar qualquer implementação de rede sem fios, é preciso realizar um estudo dos locais da rede, determinar o tipo de tráfego correspondente a entidade, necessitando da rede, etc. A seguir, é necessário determinar uma lista dos equipamentos, instalar a rede e verificar se esta funciona segundo as normas de segurança. Mas a entidade pode escolher entre várias versões. As redes de tipo IEEE 802.11a são utilizadas para obter um alto desempenho (esta versão suporte aplicações de vídeo e de voz), permitindo uma transmissão de imagens e ficheiros em grande quantidade. O IEEE 802.11b (ou Wi-Fi) tem uma utilização virada para espaços de pequena área. As redes de tipo *Hiper-Lan2* da ETSI permitem realizar as mesmas operações que as redes de tipo 802.11a. Mas, o 802.11a ganhou terreno no mercado das redes sem fios, porque surgiu em primeiro no mercado nos Estados-Unidos. O 802.11a pretende agora procurar um lugar no mercado europeu. Para isso, terá que responder a umas especificações do ETSI.

6.7 Conclusão

A norma IEEE 802.11 foi uma das primeiras normas definindo a implementação de redes sem fios e parece ser uma norma bem aceita por algumas empresas, já equipadas com redes deste tipo. Brevemente, esta rede poderá ser implementada nalgumas empresas europeias. Mas, ao nível da segurança, a norma 802.11 deverá melhorar certos aspectos. As redes sem fios deste tipo já foram por várias ocasiões atacadas. Portanto, a questão de segurança fica um problema para este tipo de redes sem fios.

Capítulo 7

DGO lança-se na aventura da WAN

Página 54, por S. Gomes da Silva

A **Direcção Geral do Orçamento**, antigamente designada por Direcção Geral Da Contabilidade Pública foi criada há cerca de 150 anos. É o serviço do **Ministério das Finanças**, integrado na administração directa do Estado, dotado de autonomia administrativa, que tem por missão superintender na elaboração e controlo da execução do Orçamento do Estado, na Contabilidade Pública e no controlo da legalidade, regularidade e economia da administração financeira do Estado. É composta por 14 delegações, afastadas umas das outras.

Normalmente uma instituição desta importância devia estar dotada de um sistema de redes e de telecomunicações fiável e equipado com novas tecnologias. A **DGO** estava, a pouco tempo atrás, equipada apenas de uma LAN. Hoje, esta instituição do Estado decidiu mudar as características das suas redes e passar a utilizar **WAN** (*Wide Area Network*).

7.1 O que é uma WAN?

Quando as distâncias são muito importantes para ligar redes locais com as suas velocidades de transmissão, é necessário a utilização de uma WAN (*Wide Area Network*). O acesso a uma rede desta, é limitado em termos de velociade de transmissão por causa das linhas telefónicas, que representam um tráfego enorme. O débito deste tipo de rede não ultrapassa os 56 Kbps. Algumas linhas especializadas dos operadores telefónicos têm um débito que não ultrapassa 1.5 Mbps.

As WAN funcionam graças a routers que permitem escolher o caminho o mais apropriado para atingir um nó da rede. Uma WAN é portanto um conjunto de LAN ligadas por routers. Existem vários tipos de rede WAN: podem ser **PSTN**, **PSDN**, **RDIS**.

Redes PSTN - *Public Switched Telephone Network*

São redes telefónicas, que utilizam um modem em cada extremo da ligação para converter os sinais digitais em sinais analógicos.

Redes PSDN - *Public Switches Data Network*

Concebidas para a transmissão de dados em vez de transmissão de voz.

Redes ISDN - *Integrated Services Digital Network*

Conversão das redes PSTN de modo a integrar dados de voz (sem necessidades de modem).

7.2 Os problemas da DGO

A passagem de LAN para WAN não se fez de um dia para o outro. Pelo contrário, a DGO teve que ultrapassar muitas dificuldades. Em 1997, nem se quer tinha um *back-up* ISDN, um sistema de *firewall*, o que é indespensável para manter a segurança no interior de uma rede, devido a ataques do exterior, nem um acesso à Internet, que é hoje muito importante, porque a Internet é considerada como maior fonte de informação. As delegações eram ligadas a partir de uma linha analógica de 9600 Kbps, o que é pouco para uma instituição desta importância. As delegações nem tinham servidores. Para ultrapassar este problema, foram implementadas linhas a 64 Kbps.

Mas com a chegada do famoso *bug* do milénio, foi necessário modificar alguns aspectos da rede, porque não se sabia o impacto que ia ter este *bug* sobre as empresas: incompatibilidade, quebras frequentes de serviço nas linhas. Os routers e as linhas foram substituidas e foram instalados *backups*. O sistema de cablagem foi repensado de uma maneira mais económica e estruturada. Em relação à *Internet*, foi desenvolvido um sistema de *e-mail*, que aumentou assim o tráfego.

A **DGO** tem por missão de autorizar as despesas do Estado. Mas estas autorizações não podiam ser comunicadas sem a existência de um sistema de rede. Daí, surge então a ideia de pedir os serviços de empresas, especializadas na instalação de WAN, para implementar um sistema mais fiável e mais potente.

7.3 Passagem de LAN para WAN

Esta responsabilidade foi confiada a Maxitel. Este projecto utiliza uma antena omnidireccional nos serviços centrais. Com esta antena, pode coexistir 15 portadores diferentes e 15 canais independentes numa amplitude de 180 graus. Esta instalação não foi realizada de um dia para o outro. Em primeiro, tiveram que estudar as linhas de vista, depois se seguiu as reuniões de negociações e finalmente a implementação do projecto.

Também ocorrerem complicações a este nível, devido orientação das antenas, è à configuração dos equipamentos. Também tiveram que resolver problemas devido a pontos de vulnerabilidade, como o exemplo indicado pelo director técnico da DGO, neste artigo: o transformador de um *switch* ardeu e as comunicações foram todas bloqueadas. O director insiste no facto, que a rede não pode depender de um único transformador. A topografia da rede (estrela) sofreu muitas alterações.

A rede funciona numa frequência de 2,4 GHz. Permite débitos de 11Mbps teóricos para distâncias de 2,5 km.

Surgiram também problemas em relação às linhas de vista, porque a superfície espalhada das torres do Instituto Técnico de Lisboa consistuem um problema para a ligação de delegações. Para remediar a este problema, foi preciso mudar a posição e a orientação das antenas.

A DGO também teve de optar pelo Windows, ao nível operacional, porque o Unix não era compatível com algumas aplicações que a DGO tinha que utilizar. A DGO também quis ter a garantia que não houvesse interferências na rede. A Maxitel, responsável pela implementação deste rojecto, garantiu que não ia haver qualquer tipo de interferência.

Para garantir a segurança no interior da rede, o sistema de encriptação escolhido foi o IPsec, com a encriptação router a router.

7.4 O futuro da rede

Até agora, não foram detectadas quaisquer falhas de comunicação. A DGO está preocupada com o futuro devido à largura de banda, que por já, podem ser suficiente, mas com certeza, que chegará o dia, em que esta largura de banda será insuficiente. Também está previsto a implementação do sistema voz sobre IP (tema abordado na revista Redes nº) e a criação de uma rede de voz e de videoconferência entre os serviços centrais e as delegações.

Com este caso, podemos nos aperceber que a implementação de uma rede WAN é muitas vezes complexa. Aparecem muitos problemas difíceis de ultrapassar. Mas para muitas instituições, este tipo de rede é muito importante para a expansão desta e para acompanhar o avanço da tecnologia.

Capítulo 8

Portugal avança nos serviços de voz

Página 57, por S. Gomes da Silva

Uma das tendências maioritária na área da telefonia é a telefonia sem fios e móvel. Se hoje em dia existe no mundo cerca de 1 bilião de linhas fixas de telefonia para 500 a 700 milhões de clientes móveis, todos concordem no facto destas curvas irão se cruzar em 2005 e que no fim desta decennia o mundo sem fios será maioritário em relação ao mundo fixo.

Há hoje em dia, no mundo inteiro, 1.5 bilião de telefones, cujo os dois terços são telefones fixos, e teremos em 2005 creca de 2 biliões de telefones, cuja metade será sempre constituída por telefones com fios. Ou seja, muito mais que os computadores pessoais, porque os telefones são utilizados por todos, enquanto os computadores constituem uma fonte de complexidade para muitos.

Constatando este aumento de telefones, alguns levantarem a seguinte pergunta: como permitir o acesso à sistemas de informação de empresas, à conteúdos e serviços da Web, às pessoas que só dispõem de telefone? Como disponibilizar esta informação para os telefones quer fixos quer móveis.

Em Portugal, são vários os serviços oferecidos pelas operadores de telecomunicações: o Projecto 118 da Portugal Telecom, projectos da INESC e também multinacionais desenvolvendo standards como o *VoiceXML* e o SALT.

8.1 VoiceXML - *Voice Extensible Markup Language*

8.1.1 História do *VoiceXML*

No meio dos anos 90, quatro pesquisadores dos laboratórios *Bell* de AT&T, Dave Ladd, Chris Ramming, Ken Rehor e Curt Tuckey tiveram uma ideia: um *gateway* equipada de um *browser* vocal que interpreta uma linguagem de diálogo para disponibilizar conteúdos e serviços *Web* a um telefone normal. Este projecto era designado "*Phone Web*". Mas, estes pesquisadores separaram-se, e cada um continuou o desenvolvimento na sua respectiva empresa.

Muitas empresas desenvolvem a sua própria linguagem. A *AT&T* desenvolve o PML (*Phone Markup Language*), a *Motorola* o "*VoxML*"e *IBM* o "*SpeechML*". Mais tarde, *AT&T*, *IBM*, *Lucent Technologies* e *Motorola* criam, em 1999, o ***VoiceXML Forum***, que dita as especificações do *VoiceXML*. A maoria das empresas trabalhando com a tecnologia vocal utilizam o *VoiceXML*. Desde o ano 2000, o standard é dirigido pelo *World Wide Web Consortium* (**W3C**). O **W3C** desenvolve standards para o *Web*, favorizando a troca de informação, o comércio, etc.

8.1.2 O que é o *VoiceXML*?

O *VoiceXML* é uma linguagem de programação para interacções vocais homens-máquinas. O *VoiceXML* é uma linguagem de *tags*, como o HTML. A diferença é que o HTML é utilizado por o *browser Web* para formatar conteúdos e o *VoiceXML* é utilizado por um *Voice Gateway*, ainda chamado *Voice Browser*. Uma aplicação desenvolvida em *VoiceXML* pode falar com um utilizador via filmes áudio pre-gravados ou de síntese de voz. Também pode receber entrada de comandos via o reconhecimento vocal ou via os códigos DTM nas teclas do telefone.

8.1.3 Aplicações do VoiceXML

- seviços que combinam o *Web* e o vocal, para permitir ao utilizador de configurar serviços que o interessa num *site Web*, e depois consultá-los periodicamente pelo telefone (tempo, bolsa, actualidade, tráfego, etc.)
- serviços de lista telefónica automatizada
- etc.

8.2 SALT - Speech Application Language Tags

Em português, **SALT** significa marcações para linguagem de aplicações de voz. Também é uma linguagem utilizando *tags*, como o HTML, que disponibi-

lizam o acesso a essas páginas através de voz, seja por telefone (fixo ou celular), microfones ligados a computadores ou dispositivos semelhantes. As marcações (tags) SALT podem ser usadas para incluir nas páginas tanto a tecnologia de reconhecimento de voz (para entrada de dados, transformando uma frase pronunciada pelo cliente em texto digitalizado a ser introduzido no aplicativo) ou para a de vocalização de textos (para saída de dados, sonorizando um texto fornecido pelo aplicativo para transmití-lo ao cliente).

Evidentemente, as marcações SALT não permitem o uso dos dispositivos de entrada tradicionais, como teclado, mouse, ou qualquer outro. Apenas inclui a voz como meio adicional. Por exemplo: usando o programa navegador de seu micro para visitar o site de uma companhia aérea, um cliente pode seleccionar o ícone das informações sobre voos com um clique de mouse e, depois, solicitar que a lista seja exibida pelo navegador falando ao microfone: "Mostre-me os voos de San Francisco para Boston depois das dezanove horas de sábado".

O exemplo acima foi obtido no próprio site do *SALT Forum* (www.saltforum.org), uma instituição criada por empresas interessadas na tecnologia de voz, entre as quais se destacam *Intel*, *Microsoft* e *Cisco*, com o objectivo de desenvolver uma especificação aberta que permita incluir entrada e saída de voz nas linguagens de marcação existentes. As principais acções do fórum se concentram em criar e divulgar técnicas de programação, que possibilitem integrar o uso da voz nas aplicações da *Internet* e padronizar o acesso via voz, possibilitando que os biliões de utilizadores de telefones, fixos e celulares, possam aceder às informações directamente na *Internet* sem necessidade de recorrer a um computador ou qualquer outro meio.

Mas, existe uma barreira para a implementação deste sistema de serviços de voz: a barreira da língua. Efectivamente, nem todos falam da mesma maneira, por exemplo, no caso do Português, "existe uma tendência a "engolir os sons", como o indica um investigador da **INESC**. Outro exemplo é a existência de sotaques. Assim, quando a máquina não conhece um som, esta não efectua nenhuma operação. Portanto para remediar a esta barreira, é necessária a existência de uma vasta biblioteca de palavras e sons. Esta operação demora tempo a ser implementada. Um projecto que é constituído por uma vasta biblioteca é o **projecto 118**, serviço disponível para os clientes da **Portugal Telecom**.

8.3 Projecto 118 da Portugal Telecom

Quando se pede a uma operadora do serviço 118 da Portugal Telecom (PT), um determinado número de telefone ou morada, a resposta surge breve e numa voz bem modulada. De intervenção humana, existe apenas o primeiro contacto com a operadora. A voz de resposta foi gravada e a articulação das palavras ou números é feita por via informática. O lado audível do 118 "esconde"uma base de dados com mais de quatro milhões de registos, para suporte de cerca de

70 milhões de chamadas por ano. Nos períodos de maior tráfego, atinge-se um "pico"horário de 25 mil chamadas. O tempo de reposta da pesquisa é inferior a meio segundo e o sistema suporta mais de 500 operadores em simultâneo. A "espinha dorsal"do serviço 118 da Portugal Telecom é um projecto/produto que começou a ser desenvolvido há cerca de 9 anos por uma equipa do INESC, hoje integrada na **Link**, em parceria com a **PT Inovação** e a **Philips**. O *hardware* e um sistema de gestão de base de dados foram configurados. Foi também desenvolvido um motor de pesquisa - um servidor aplicacional que faz a interface entre as aplicações e a base de dados; tudo com base em equipamentos e tecnologias standard. Foi a própria PT que exigiu que os equipamentos utilizados fossem genéricos, de baixo custo e facilmente actualizáveis.

O **Projecto 118** utiliza servidores em **Unix**, está dotado de uma base de dados relacional e utiliza como linguagem de programação C, C++ e Java. A nível da tecnologia genérica, o sistema utiliza ainda interfaces alfanuméricos e *Windows*, IVR (*integrated voice response* - estes sistemas automatizam interações telefónicas de todos os tipos, suportando igualmente reconhecimento de fala) para a informação dos números e dos nomes. A nível das comunicações utiliza-se a *Internet*, **TCP/IP** para a LAN/WAN. Na arquitectura do sistema desenvolvido pela Link poderão ser identificados três níveis distintos: servidores de base de dados, servidores aplicacionais e interfaces cliente. O sistema possui dois ou mais servidores de bases de dados em localizações distintas, para prevenção de falhas num centro de processamento. Do mesmo modo, existem dois ou mais servidores aplicacionais que garantem a gestão optimizada dos recursos dos servidores de bases de dados, com capacidade de detecção da sua disponibilidade de modo a garantir a tolerância a falhas. O sistema tem também uma configuração para distribuição de carga entre os vários servidores - suportando falhas de vários equipamentos a vários níveis - quer por configuração automática nos clientes quer por configuração automática nos servidores aplicacionais. A nível da gestão de base de dados, foi implementada a replicação de dados entre os vários servidores de BDs por forma a assegurar a coerência dos dados e a tolerância a falhas.

8.4 Implementação destes serviços

Uma vez que o sistema reconheceu a opção do cliente, basta então reencaminhar a chamada para o operador que a partir da opção atribui a informação correspondente. Se a empresa pretende implementar um sistema de síntese de voz, então o servidor será constituído de uma plataforma com interface telefónico, de um servidor para reconhecer os sons e de um servidor para síntese de voz.

Em Portugal, já existem serviços de voz implementados. Mas, o desenvolvimento de um tal serviço é custoso e complexo, mesmo com a existência de standards de voz. O problema não vem da implementação, mas sim da criação de uma vasta biblioteca, que são soluções demoradas.

Capítulo 9

P2P desperta atenções

Página 33, por F. Rocha

O modelo de utilização da *Internet* centrado na *Web* e nos *browsers* parece mostrar sinais de esgotamento. Uma segunda fase começa a emergir em torno de uma tecnologia, o da conexão pessoa-a-pessoa, tecnologia que já existe há vários anos, conhecido como o ***Peer-To-Peer*** ou P2P. Muitas vezes, apresentado como una nova tecnologia, o *peer-to-peer* não tem nada de novo, já que é um conceito tão antigo como o sistema informático distribuído. Há cerca de 30 anos, muitas companhias já estavam a implementar arquitecturas, que hoje são conhecidas com o nome *peer-to-peer*. À origem, a *Internet* era concebida como um sistema *peer-to-peer*. O objectivo de uma rede ***Arpanet*** (fundador do sistema de rede *Internet*) era de permitir aos universitários de partilhar recursos informáticos pelo território americano. Muito antes de ser uma infra-estrutura cliente/servidor, a *Internet* era inicialmente concebida para a comunicação entre máquinas partilhando recursos.

Esta tecnologia tornou-se popular com o *Napster*, que consista na troca de dados (música, imagens, vídeos, etc). Mas esta proposta acabou por ser interrompida devido ao facto desta ser ilegal, embora tenha obtido um certo sucesso por parte dos jovens utilizadores.

A tecnologia ganhou agora um novo rumo. Efectivamente, o P2P está agora a levantar interesso por parte das empresas. As utilizações deste tipo de tecnologia poderão permitir às empresas de reduzir os custos elevados, devido ao número elevado de ligações efectuadas através de *Wide Area Networks* (WAN), evitando assim a passagem de dados por equipamento de rede. Mas, alguns especialistas garantem que esta tecnologia não irá interferir no mercado das LAN e das WAN e deverá ser considerada pelas empresas como um complemento a estes tipos de rede.

9.1 O que é o *Peer-To-Peer*

Na *Internet*, encontramos do lado dos clientes, aplicações instaladas na máquina do utilizador para utilizar diferentes serviços IP: *mail*, *Web*, etc. Do lado dos servidores, encontram-se programas instalados em máquinas potentes que disponibilizam um ou mais serviços ao cliente. Esta arquitectura é designada arquitectura **cliente/servidor**.

Pelo contrário, no ambiente P2P, todos os utilizadores são clientes e servidores ao mesmo tempo. Concretamente, através da arquitectura P2P, cada utilizador pode partilhar e gerir recursos como lhe apetecer: definição das autorizações sobre ficheiros, elaboração das estruturas de acesso à informação. Já não existe servidor central para armazenar e gerir os dados, mas a informação é partilhada para diferentes máquinas.

9.2 A arquitectura centralizada

Quem nunca ouviu falar do **Napster**? Um serviço *Peer-To-Peer* especializado nas trocas de ficheiros áudio que contribuiu para o desenvolvimento da tecnologia P2P no mercado público e mesmo professional. A originalidade deste tipo de rede, virado agora para o sector comercial, consiste na adopção de uma **arquitectura centralizada**. Um tal dispositivo representa actualmente a solução a mais confortável para partilhar ficheiros numa comunidade. Mas, na realidade, este tipo de arquitectura exige um investimento tal, em recursos, que os serviços ficam raramente de boa qualidade.

Concretamente, numa arquitectura centralizada, um dispositivo exclusivamente servidor encarrega-se de estabelecer uma ligação directa entre os utilizadores ligados ao servidor. O interesso desta técnica é a indexação centralizada de todos os ficheiros partilhados pelos utilizadores da rede. Esta indexação é útil para fornecer ao cliente cartografia dos recursos disponíveis: quando uma pesquisa é efectuada, os ***peers*** (utilizadores da tecnologia P2P) podem comunicar entre si sem a necessidade de assistência do servidor central. Cada vez que um utilizador efectua uma pesquisa para um determinado ficheiro, o servidor central cria uma lista dos ficheiros correspondentes à pesquisa, verificando na base de dados do servidor, os ficheiros pertencentes a utilizadores conectados. O servidor central afixa a lista. O cliente pode assim seleccionar os ficheiros desejados a partir da lista e estabelecer uma ligação directa com o computador individual que detém o ficheiro. O *download* efectua-se directamente entre um utilizador e um outro. A figura seguinte representa a arquitectura do P2P centralizado.

Uma das principais vantagens deste modelo é a indexação central que permite localizar rapidamente os ficheiros, graças a base de dados regularmente actual-

izada pelo servidor. Nesta configuração, todos os clientes são obrigados a estar ligado à rede do servidor, a pesquisa atinge todos os utilizadores conectados.

Mas também existem desvantagens deste modelo centralizado. Este tipo de sistema só permite a entrada no sistema por um único ponto: o servidor central. Apenas bastava bloquear o servidor para desligar todos os utilizadores da rede e para o funcionamento do conjunto da rede. Outra desvantagem de utilizar uma arquitectura centralizada é o facto que uma pessoa que se liga à rede, tem que efectuar um registo, perdendo então o anonimato. O servidor conhece o endereço IP da máquina e o tipo de ficheiros que estão a ser processados. Por fim, a troca de ficheiros numéricos a grande escala na *Internet* (música, vídeo, photo, etc.) provoca o não-respeito das protecções intelectuais. As obras registadas com *copyright* circulam nas redes P2P, o que corresponde a uma organização de piratagem.

9.3 A arquitectura descentralizada

O segundo modelo utiliza um sistema de nós de redes, em vez de utilizar um servidor central. O cliente do programa liga-se via *Internet* ao computador de um ou mais utilizadores, o conjunto constituindo a rede. Assim, cada um dos utilizadores põe a disposição ao conjunto da comunidade, uma parte dos ficheiros do seu computador. O princípio da ligação é o seguinte: um computador "A", equipado com um programa específico, se conecta a um computador "B", também equipado com o mesmo programa. "A"anuncia a sua presença a "B". "B"comunica esta informação a todos os computadores aos quais está ligado, "C", "D", "E"e "F". Por sua vez, estes computadores comunicarão esta informação aos computadores aos quais estão conectados. E assim seguidamente com o resto da rede.

Uma vez que a máquina faz parte integrante da rede, o cliente pode efectuar uma pesquisa. Assim, "A"efectua a sua pesquisa começando por "B", este que efectua a mesma pesquisa em "C", etc.Mas existe uma diferença fundamental: quando o cliente valida uma pesquisa, esta fica sempre activa e o seu tratamento nunca para. Este modelo é muito mais robusto, porque o sistema não depende de um servidor central. A arquitectura descentralizada é representada na figura seguinte:

Este tipo de sistema oferece muitas vantagens. Em primeiro, porque é descentralizado e não pode desaparecer de um dia para o outro. Isto significa que ninguém é indispensável para o bom funcionamento do dispositivo. Outra vantagem ou desvantagem (depende dos pontos de vistos) é o anonimato, porque não existe nenhum sistema central para recuperar os dados pessoais. Também não existe qualquer restrição em relação aos ficheiros procurados.

9.4 O futuro do *Peer-To-Peer*

O P2P parece levantar muito interesso por parte das empresas. Mas já foi referido, uma empresa não se pode limitar a este tipo de rede. O P2P pode substituir algumas ligações WAN, reduzindo assim os custos que estas redes implicam. Mas ainda existe um ponto para resolver: a segurança. A segurança também é um ponto importante nas redes tradicionais, que utilizam *browsers*. Mas, nas redes *Peer-To-Peer*, este problema é ainda mais importante, particularmente se um cliente desta rede desejar autenticar aqueles se estão ligados e assegurar a segurança das trocas de dados. Sem ferramenta de administração, a informação é duplicada e transmitida a cada um dos nós da rede, sem nenhum controlo.

Para remediar aos problemas de segurança, os *firewalls* são ferramentas ideais para filtrar os pacotes de dados. Mas esta ferramenta só permite impedir a uma parte da rede de comunicar com a outra parte. Na maioria das vezes, este sistema permite a passagem de fluxos para o exterior, mas proíba o tráfego para o exterior. Os *firewalls* permitem ligações exteriores via HTTP (porto 80). Este sistema provoca problemas, porque certas aplicações são transmitidas através deste porto, o que torna o sistema mais frágil aos ataques de vírus.

Portanto, para aplicar este tipo de rede às empresas, será necessário encontrar novas soluções de segurança. Mas o P2P também começa a interessar, não só as empresas, mas também alguns fornecedores, como a *SUN*, a *Intel*, a *Novell* e a *Groove Networks*, com os respectivos produtos, **Jxta** da Sun, **Share and Learn** e **NetBatch** da Intel e **Groove** da Groove Networks. O *Peer-To-Peer* parece ter um futuro garantido no sector empresarial, que depende de algumas funções de deverão ser melhoradas.

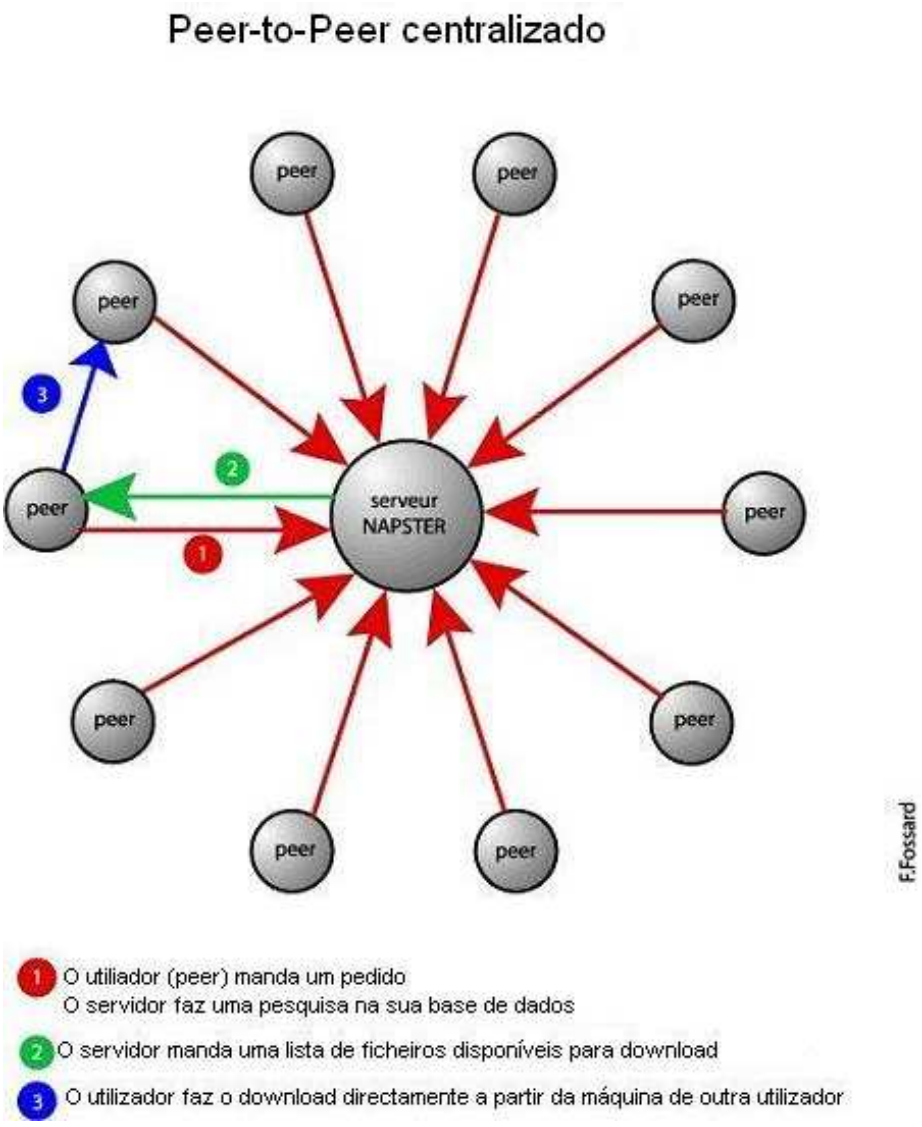

Figura 9.1: Arquitectura do P2P centralizado

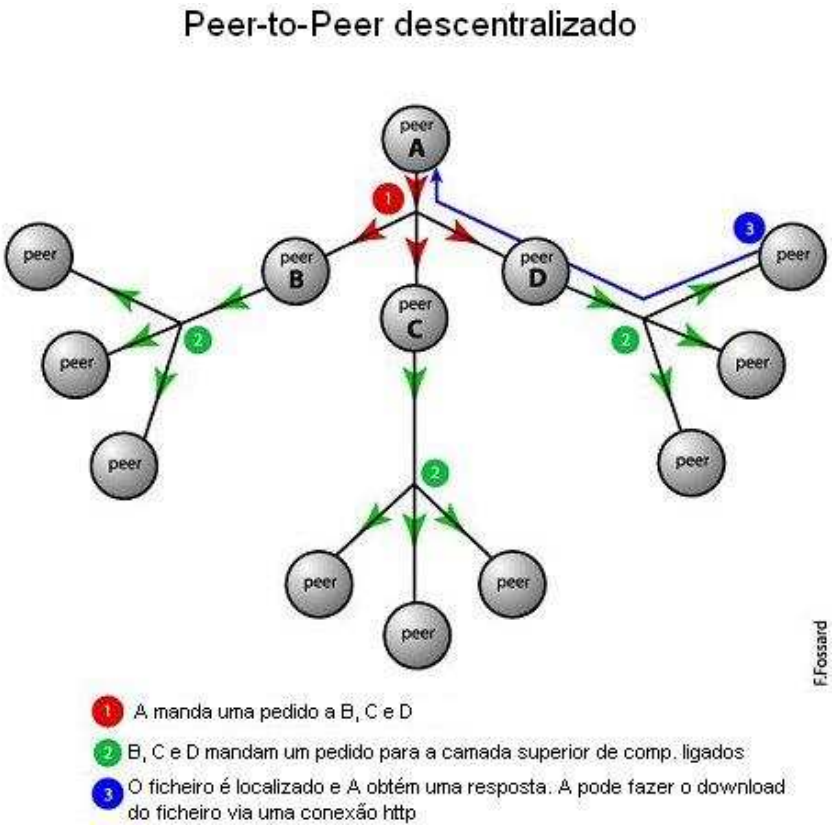

Figura 9.2: Arquitectura do P2P descentralizado

Capítulo 10

Outros temas abordados na revista

Nesta secção não serão comentados os artigos, mas apenas explicados alguns temas.

10.1 ADSL, página 28

O **ADSL**, *Asymetric Digital Subscriber Line* (em português Linha Digital Assimétrica para Assinantes), não se refere às linhas telefónicas, mas sim aos modems utilizados. Esta tecnologia aproveita toda a rede telefónica, permitindo altos débitos no par de cobre da linha, e é instalada para transmitir e receber sinais digitais em alta velocidade. Os débitos são de 10 a 25 vezes mais elevados dos que são utilizados num modem de 56K tradicional.

O sistema consiste em dividir a linha telefónica em 3 canais virtuais (1 canal para Voz, 1 canal de alta velocidade para Download e 1 canal duplex de velocidade média para Upload) as velocidades de *download* podem ir de 256K até 6.1 Mbps e de *upload* de 16k até 640K, por isso ela é assimétrica (velocidade maior para *download* e velocidade menor para *upload*)

A comunicação é feita da seguinte forma: os dados do seu computador são enviados para o modem, que converte os sinais digitais em analógicos e envia para a central telefónica através da sua linha telefónica. O sinal depois de enviado para a central telefónica é novamente separado e os dados vão para um equipamento DSLAM (DSLAM - *Digital Subscriber Line Access Multiplexer*), o DSLAM limita a velocidade do utilizador, uni várias linhas ADSL e envia para uma linha **ATM** de alta velocidade, esta conectada a Internet.

Como as frequências utilizadas pelo ADSL, para o tráfego de dados, são diferentes das frequências das chamadas de voz, é permitida a utilização simultânea do telefone/fax enquanto se navega na *Internet*.

10.2 VPN, página 28

Virtual Private Network (VPN) ou Rede Privada Virtual é uma rede privada (rede com acesso restrito) construída sobre a infra-estrutura de uma rede pública (recurso público, sem controlo sobre o acesso aos dados), normalmente a *Internet*. Ou seja, ao invés de se utilizar links dedicados ou redes de pacotes para conectar redes remotas, utiliza-se a infra-estrutura da *Internet*, uma vez que, para os utilizadores, a forma como as redes estão conectadas é transparente.

A principal motivação para implementação de VPNs é financeira: links dedicados são caros, principalmente quando as distâncias são grandes. Por outro lado existe a *Internet*, que por ser uma rede de alcance mundial, tem pontos de presença espalhados pelo mundo. Conexões com a Internet podem ter um custo mais baixo que links dedicados, principalmente quando as distâncias forem grandes. Por que então não utilizar a infra-estrutura da Internet para conectar a rede privada? É essa a principal motivação das VPNs.

Utilizar a Internet como a infra-estrutura para conectar redes privadas é uma ótima solução em termos de custos mas.Mas, a Internet é uma rede pública, onde os dados em trânsito podem ser "lidos"por qualquer equipamento. Como fica então a questão da segurança e em especial a confidencialidade das informações circulando?

Para incorporar segurança na comunicação entre as redes privadas é necessária uma maneira de trocar dados criptografados (codificados) de forma que, se os dados forem capturados durante a transmissão, não possam ser decifrados. Os dados circulam criptografados pela Internet em "túneis virtuais", criados por dispositivos VPN que utilizam criptografia; e esses dispositivos que são capazes de "entender"os dados criptografados formam uma "rede virtual"sobre a rede pública. É essa rede virtual que é conhecida como VPN.

Os dispositivos responsáveis pela formação e gestão dessa rede virtual, para garantir uma comunicação com segurança, devem ser capazes de garantir:

- Privacidade dos dados, ou seja, caso os dados sejam interceptados durante a transmissão, não podem ser descodificados.
- Integridade dos dados, além de não serem descodificados (privacidade), os dados não podem ser modificados durante a transmissão.

- Autenticação, garantia de que os dados estão sendo transmitidos ou recebidos do dispositivo remoto autorizado e não de um equipamento qualquer, ou seja, garantia que o dispositivo remoto com o qual o túnel foi estabelecido é o dispositivo remoto autorizado e não outro equipamento se "fazendo passar por ele".

Este tema é abordado em profundidade na revista Redes nº89 , portanto não iremos insistir muito na estrutura da VPN.

10.3 SSL, página 63

Secure Sockets Layer (SSL), elaborada pela *Netscape Communications*, é um protocolo de encriptação, que trabalha a baixo nível, utilizado para encriptar as transacções de protocolos de níveis superiores: HTTP, FTP, etc. É uma tecnologia padrão de segurança para se criar uma conexão criptografada entre um servidor *web* e um *browser*. Esta conexão assegura-se de que todos os dados transmitidos entre o servidor e o *browser* permanecem confidenciais e íntegres. O SSL é um padrão da indústria e é usado por milhões de websites em suas transacções seguras com os seus clientes. Para poder gerar uma ligação com SSL, o servidor necessita de um Certificado SSL.

Inclui mecanismos de autenticação do servidor (verifica a identidade do servidor), a encriptação dos dados que circulam na rede, e a autenticação do cliente (verifica a identidade do cliente).

O SSL é implementado nos *browsers Netscape* e *Internet Explorer*, e em muitos outros browsers.

Conclusão

Este trabalho que nos foi proposto para a cadeira de Redes de Dados, foi um trabalho de investigação muito interessante para adquirir conhecimentos em relação à redes de dados.

Nesta revista, foram abordados muitos temas relacionados com o mercado actual, como por exemplo o standard 802.11x e o Peer-to-Peer. Reparamos que estes produtos estão agora a procurar o seu lugar no sector das redes.

O wireless parece ser cada vez mais utilizado por pessoas que necessitam de se mover. Alguns standards já foram aplicados a redes sem fios, mas infelizmente, ainda falta alguns pormenores que deverão ser rectificados para o sucesso destes standards, como por exemplo o problema da insegurança destas redes. Efectivamente, o pessoa equipado com os mesmo material, pode se conectar à rede, se esta não está previamente equipada de um sistema de autenticação.

Também foi constatado que Portugal está no bom caminho nos servidores de voz, já com alguns sistemas instalados. Mas ainda precisa de efectuar alguns esforços neste sentido.

Acho que este trabalho foi bastante benéfico para mim, porque fiquei com muito mais conhecimentos no domínio das redes de dados, sobretudo, porque fiquei a conhecer muitos projectos que não conhecia e também nos obrigou a pesquisar muita informação para a realização do trabalho.

Bibliografia

[1] www.siemns.com

[2] www.tele.ntnu.no/users/andrew/MPEG/uma

[3] www.commentcamarche.fr

[4] www.sowap.com/wap-faq.html

[5] www.networkdesigners.com.br

[6] www.3com.com

[7] news.zdnet.fr/

[8] xmlfr.org/actualites

[9] www.xmlforum.org

[10] solutions.journaldunet.com/0104/010424 _eai.shtml

[11] www.janelanaweb.com/digitais/p2p.html

[12] www.dgo.pt

[13] www.pdacool.com

[14] www.w3.org/

[15] solutions.journaldunet.com/0201/020129 _jca.shtml

[16] www.abou.org/p2p

[17] www.zdnet.fr/techreport/peer-to-peer

[18] www.dexem.fr/education.html

[19] www.dexem.fr/faq.html

[20] www.link.pt

[21] www.bpiropo.com.br

[22] www.lifl.fr/ boulet/formation/syst-dist/exposes2000-2001/bluetooth/site /rapport.htm

[23] www.guill.net/reseaux

[24] Sebenta de Redes de Dados I, *Gabriel Pires*

[25] fr.news.yahoo.com/021003/60/2s1nr.html

[26] www.argonavis.com.br

[27] www.novis.pt

[28] www.cyclades.com.br

[29] planeta.terra.com.br/negocios/fernando.toshio/adsl.htm

[30] amalia.img.lx.it.pt/ fp/st/ano2001_02/trabalhos2001_02/trabalho3/ADSL_Web /o_que_e_adsl.htm